A REPORTER AT LARGE

THE COLD WAR BUNKER THAT BECAME HOME TO A DARK-WEB EMPIRE

An eccentric Dutchman began living in a giant underground facility built by the German military—and ran a server farm beloved by cybercriminals.

By Ed Caesar

July 27, 2020

In the mid-nineteen-seventies, the West German military, the Bundeswehr, built a vast underground bunker near the town of Traben-Trarbach. It was five stories deep, had nearly sixty thousand square feet of floor space, and was designed to withstand a nuclear attack. Eighty days' worth of survival provisions were stored inside, including an emergency power supply and more than a million litres of drinking water. You entered the facility through an air lock; the interior temperature was set to seventy degrees. The walls were concrete, thirty-one inches thick, and some were lined with copper. The rooms were soundproof and transmission-proof. Between 1978 and 2012, the bunker was the headquarters of the Bundeswehr's meteorological division, and at any one time about three hundred and fifty civilian contractors worked there; most of them focussed on predicting and plotting weather patterns wherever the German military was deployed. New employees often got lost. On each level, the walls were painted a different color, to help people orient themselves—but the bunker was symmetrical, so one side looked much like another. There was no natural light. In winter, workers on day shifts arrived in the dark and left in the dark.

In 2012, the Bundeswehr moved its meteorological division to another site. Germany's federal real-estate agency, known as BImA, listed the bunker for three hundred and fifty thousand euros. The low price reflected the unusual nature of the property and the expense of maintaining it. The bunker sat beneath a plot of some thirty acres, in a forested area on a hill outside Traben-Trarbach, which is an hour east of the Belgian border. The perimeter of the property was marked by ramparts and a fence, and aboveground the site contained several large structures, including a gatehouse, an office building, a

tall aerial with satellite dishes, a helipad, and barracks constructed by the Nazis in 1933. The Bundeswehr had employed twelve men, who worked in shifts around the clock, solely to insure that the bunker was properly ventilated and did not flood. The German government hoped that a technology business, or perhaps a hotel, might want the premises, but there were few prospective buyers.

The relocation of the Bundeswehr division was a blow to the local economy. Traben-Trarbach is a fairy-tale town that straddles a bend in the wide, teal-blue Mosel River. Traben is on the north bank, Trarbach on the south. The town, which is overlooked by a ruined fourteenth-century castle, is full of aesthetic quirks and highly caloric delicacies. Only about six thousand people live there, but thousands of tourists arrive every summer to hike, drink the local Riesling, and take river cruises. At the turn of the twentieth century, Traben-Trarbach was a wine-trading hub second only to Bordeaux, and also a center of the Jugendstil movement, the German iteration of Art Nouveau; many of its buildings reflect the wealth and the brio of that period. Near the hotel where I stayed in December, a Jugendstil relief of Rapunzel adorned the side of an apartment building. Her gilded hair fell in wavy lines from the fourth floor to the second.

The mayor of Traben-Trarbach, Patrice-Christian-Roger Langer, a garrulous man with a fine gray beard, worked at the bunker complex for nearly thirty years, and for eleven of them he operated its mainframe computer. He enjoyed his time working underground. But, he told me, "not everybody could deal with working in a bunker," adding, "It's a mental thing . . . if you don't have a *window*."

In 2012, a foundation controlled by a fifty-three-year-old Dutchman named Herman-Johan Xennt proposed to buy the bunker complex. Xennt travelled to Traben-Trarbach to explain his plans to a closed session of the town council. He was a striking man, with a cascade of shoulder-length gray-blond hair, and wore a dark suit, which highlighted the pallor of his face. Xennt told the council that he intended to set up a Web-hosting business at the bunker complex, and

promised to create as many as a hundred jobs for local people, but he was vague when pressed for details.

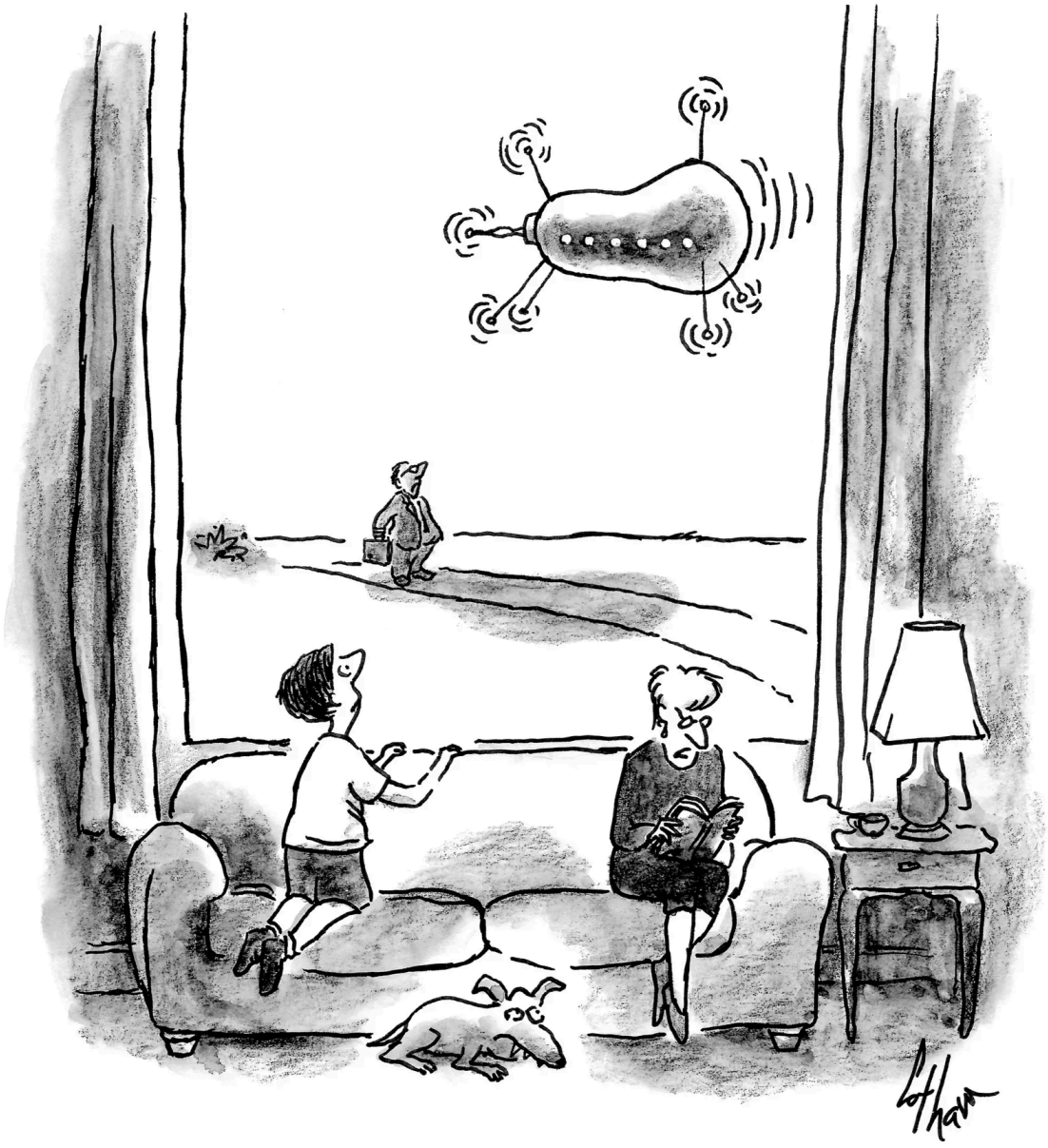
Several council members were concerned about Xennt's credentials. Although he said that he had been in the Web-hosting business for years, he did not name any blue-chip clients. But there were no other viable buyers, and so, in June, 2013, the property was sold to Xennt's foundation. One of the council members, Heide Pönnighaus, later told a newspaper, "I didn't have the best feeling about it."

Xennt was born Herman-Johan Verwoert-Derksen, in 1959. He grew up in Arnhem, a small city in the eastern Netherlands which had been the site of intense fighting during the Second World War. As a teen-ager, he became interested in historical buildings, and several times he visited an old Nazi bunker on the edge of town. He also fell in love with science fiction, and began calling himself Xennt (pronounced "Zent"). When "Star Wars" was released, in 1977, he was enraptured by it. He decorated his bedroom to look like a spaceship, with blacked-out windows, jury-rigged electric doors, and speakers playing moody synthesizer music. In one corner of the room was an Apple II personal computer.

By his early twenties, he had officially changed his surname. Nothing irritated him more than being called by his given name, and he preferred to be called by his new surname alone. Even his parents knew him simply as Xennt. After graduating from college, in the early eighties, he started several personal-computer businesses in the Netherlands. A poster for a store that he owned, PC International, shows him with long brown hair, bushy eyebrows, and an unconvincing mustache. He is wearing a T-shirt with "Xennt" printed on it, and is standing behind a bulky monitor emblazoned with the store's logo. During this period, he and a partner, a woman of Dutch Antillean heritage named Angelique, had two sons. They named them Xyonn and Yennoah: X and Y. Xennt and Angelique soon separated, and she retained primary custody of the boys. (Xennt also has a son who was born in 2019, to a different mother.)

In 1995, when Xennt was thirty-five, he bought a twenty-thousand-square-foot former NATO bunker in the Dutch town of Goes, near the North Sea coast. The bunker, built forty-one years earlier, had ceased being used for military purposes in 1994. Xennt settled in with some old friends, including Paul Scheepers, a computer technician with a bald pate, long curly hair, and a sweet laugh. Scheepers is now fifty-eight years old, and works in I.T. support for a Dutch badminton foundation, but he still introduces himself by the online sobriquet that he adopted in the eighties: Cytrax. "We were looking for some space to make a kind of futuristic environment," Scheepers told me recently. "And what do you do when you have a bunker and you have a computer company? You put computers in the bunker."

At the Goes property, Xennt started a new business, called CyberBunker, which offered "bulletproof hosting" to Web sites. All Web sites must be physically hosted somewhere, whether on a personal computer or a server; hosting is now a multibillion-dollar industry dominated by such companies as Amazon Web Services and GoDaddy. CyberBunker offered, for a steep price, a highly secure hosting environment for sites containing sensitive, or illicit, material. In the late nineties, most of CyberBunker's customers ran pornographic sites. Xennt had a liberal outlook, but there were lines he would not cross. According to CyberBunker's Web site, its servers would host all content except "child pornography and anything related to terrorism."



"The pear-shaped object approaching the house isn't your father?"

Cartoon by Frank Cotham

Open cartoon gallery

I spoke to a former pornography distributor who used Xennt's servers during this period. (He did not want me to publish his name, as he now works in finance.) He told me that his business brought in about a million euros a year, but that Xennt himself had relatively little money, because he had imprudently bought hundreds of servers—an investment in infrastructure that took several years to pay off.

A curious mixture of adolescent-male fantasia and techno-anarchist utopia, CyberBunker anticipated the current trend for apocalypse-ready hideaways owned by the rich and paranoid. The pornographer visited the Goes facility several times. Xennt's taste in interior design had changed little since he had decorated his teen-age bedroom: the bunker was furnished with computer terminals, black leather sofas, neon-red lamps, and artificial plants. Ethereal music was often playing. The pornographer found the bunker's atmosphere strange but "impressive"; its denizens were "alternative" people. Xennt had an odd diet. For breakfast, he ate *frikandel*—a skinless, deep-fried pork sausage, which is a popular snack in the Netherlands—along with an assortment of vitamins. "Xennt was a mysterious guy," the pornographer told me, laughing. Two other former colleagues remember that the Goes bunker had a "porno room" where there were sometimes live sex shows involving Xennt's girlfriends.

In 1999, a young programmer named Sven Kamphuis, who went by the online handle CB3ROB, joined the CyberBunker collective. Kamphuis worked a day job at the Dutch Internet firm XS4ALL. He had unruly black eyebrows and a crazy mop of black hair, and his colleagues at XS4ALL thought that he looked like Bert, from "Sesame Street." They also remember him as rude, childish, and prone to conspiracy theories. But Kamphuis's talent for programming was undeniable. He soon became one of Xennt's lieutenants.

At around the same time, Xennt rented part of the bunker to another group. On July 27, 2002, there was an explosion in that section, and in the fire that ensued Xennt suffered burns on his hands and his face. The police showed up, and in the charred ruins of the bunker they found the remnants of a laboratory for making Ecstasy. Xennt's business license was taken away, but he was not charged with any crime. He maintained that he had known nothing about the drug factory, and that the subletting group had assured him it was a painting company. CyberBunker's servers were moved to aboveground facilities, in Amsterdam and elsewhere.

Xennt encouraged the notion that CyberBunker was more than a business. Less than a week after the fire, on August 1, 2002, he and Kamphuis published a declaration of independence for a new state, which they called the Republic of CyberBunker. Citing a U.N. Security Council resolution from 1960, which said that "all people have the right to self-determination," the Republic of CyberBunker—population six—seceded from the Netherlands. CyberBunker declared as its sovereign territory the five hundred acres containing the ruined bunker. The country's official currencies would be gold, dollars, and euros, and each resident would pay a flat tax of fifteen thousand dollars a year. Unusually for a republic, it had a royal family. Its President was His Majesty King Xennt von CyberBunker, and its minister of foreign affairs and telecommunications was His Royal Highness Prince Sven Olaf von CyberBunker-Kamphuis.

Kamphuis often acted as CyberBunker's spokesperson, and he promoted anti-authoritarian, libertarian ideas. Among his tenets: free speech is supreme; everyone has a right to be online; the Internet erases the power of the state; copyright is twentieth-century bullshit. Such notions were in fashion during the nineties, when big technology firms had yet to dominate the Internet. In 1996, John Perry Barlow, the anarchist writer and a founder of the Electronic Frontier Foundation, a group committed to digital freedom and privacy, wrote an influential manifesto that began, "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of the Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."
Several people told me that Xennt was not entirely sincere about his self-proclaimed regal status. (He recently called CyberBunker's declaration of independence "a joke.") But Kamphuis was serious about it—and remains so. Since 2002, he has more than once claimed to "enjoy personal and functional immunity" when faced with arrest, on charges ranging from driving offenses to cybercrime. Paul Scheepers, Xennt's longtime friend, told me that Xennt's world view was more pragmatic than Kamphuis's: he simply wanted the freedom to pursue his own projects without interference. Xennt declined to be interviewed for this article, but agreed to give written answers to a dozen

questions. He explained, "I am not interested in politics at all. I value privacy and I am against the 'big brother' policy of large corporations and governments."

In the nineties and two-thousands, however, Xennt took part in some activism, helping to instigate what became known as the Public Root movement. He and an international group of investors and programmers tried to create their own roster of top-level domains—the suffixes that follow an Internet address, such as ".org," ".com," and ".edu." They came up with various new domains—including ".schiphol," the name of Amsterdam's airport, and ".sex"—with the aim of selling them. Top-level domains are controlled by an American nonprofit organization called ICANN. At a time when the structure of the Internet still seemed to be in flux, Xennt and others in the Public Root movement chafed at ICANN's authority. In 2005, Xennt filed a patent application related to top-level domains, writing, "We state that each Internet user has the right to see all of the Internet."

The Public Root movement eventually fell apart, because of internal arguments over control, funding, and transparency. Martijn Burger, one of Xennt's former partners in the project, successfully sued Xennt for breach of contract. Burger told me that Public Root was "ideological," but added, "We also wanted to make some money."

Burger, who now works in private health care in the Netherlands, told me that Xennt has "brilliant ideas, but he's not a businessman." Peter Olsthoorn, a Dutch investigative journalist who has covered Xennt and CyberBunker ever since the Public Root contretemps, said that Xennt was an "old-fashioned anarchist" with a specific gift: he understood "the Internet in its root, in the core." Scheepers told me that Xennt was an inspired designer who might have worked for Apple had he chosen a different path.

Another former colleague of Xennt's, a Dutch programmer named Frank Van der Loos, occasionally performed legal work for CyberBunker, despite having only paralegal qualifications. When we met in The Hague in March, Van der

Loos wore a Bluetooth earpiece the entire time and spoke so quickly that I frequently misunderstood him. (He often finished his sentences with "Do you understand?") Van der Loos said that he and Xennt had argued about money, adding that Xennt's great weakness was that he was a "cheapskate." But Van der Loos also compared him to Steve Jobs. Although Xennt could code only in the rudimentary language BASIC, he was prescient about the kinds of change that a connected world would bring. Before PayPal became popular, for instance, Xennt had attempted to start his own online encrypted banking-transfer service, named Bank66. It had failed because of Xennt's greed and lack of business acumen, Van der Loos said. Nevertheless, he called Xennt "a visionary."

Jörg Angerer, a senior German prosecutor, first heard that Xennt's foundation had bought the Traben-Trarbach bunker in the summer of 2013, after a council member conveyed his concerns to the local police. Angerer, who is based in Koblenz, an hour northeast of Traben-Trarbach, is a lean and affable man with a shaved head and an unshaven face. For the past few years, his office has specialized in prosecuting cybercrime. Soon after he began researching Xennt and his company, he told me, he concluded that some of CyberBunker's clients were manifestly illegal. But CyberBunker itself appeared to exist in a gray area between activism, business, and criminality.

In the two-thousands and twenty-tens, CyberBunker and Kamphuis's associated Internet-service provider, which was also called CB3ROB, had become notorious for hosting the spam e-mail operations of phishing sites—fraudulent criminal enterprises that lure people into disclosing their credit-card details—and of rogue pharmaceutical peddlers. At the same time, CyberBunker hosted WikiLeaks, the renegade operation devoted to exposing secret documents. (Xennt told me that this was not a political gesture on his part: "CyberBunker hosted WikiLeaks indeed. Why? Because WikiLeaks hired its services.") The Pirate Bay, a site for sharing movies and other copyrighted content, was a CyberBunker client until 2010, when the Motion Picture Association of America won a court ruling, in Hamburg, that forced Xennt and Kamphuis to remove the site from its servers. Kamphuis was indignant about

the decision, telling a reporter, "Help us put these dinosaurs out of their misery!"

As Angerer continued to research CyberBunker, he learned that it could be very aggressive. Around 2010, the Spamhaus Project, a European volunteer-driven organization whose goal is to impede spammers, had begun listing I.P. and real addresses associated with CyberBunker and CB3ROB, and had lobbied Internet-service providers to block the company. In early 2013, this pressure led to CB3ROB's services being briefly taken off-line. In retaliation, Kamphuis and a loose group of hackers in different countries, who called themselves the Stophaus Collective, hit Spamhaus with a distributed denial-of-service attack, which incapacitates a site by overloading it with traffic. Kamphuis was arrested shortly after the attack, but Xennt was not; he proceeded with moving into the Traben-Trarbach bunker.

Angerer told me that he didn't fully understand Xennt's acquisition of the property, except to say that he evidently had "a weak spot for bunkers." CyberBunker gained some mystique by operating out of a fortified underground facility, but there is little benefit for customers in physically protecting servers to such an extreme degree. Moreover, the ostentatiously secure location was bound to attract the suspicion of law enforcement. Xennt's promise of bulletproof hosting, Angerer suggested, could have been more effectively fulfilled by using regular servers in a more permissive jurisdiction, such as Russia.

Xennt's desire to live and work underground was not entirely rational. Van der Loos, the former associate, told me that Xennt was *bunkergeil*—a Dutch portmanteau that means "horny for bunkers." After the underground facility in the Netherlands was destroyed by fire, in 2002, Xennt concluded that the most likely country where he might find a replacement was Germany, which had many military hideouts from the Cold War era. In 2007, Van der Loos and Xennt visited a former NATO bunker in Börfink, a facility that had been used as a center for West German intelligence in the seventies and eighties. In some areas of the Börfink bunker, there were no lights, and so the two men toured the

cavernous space in darkness, following fluorescent green arrows on the walls, like Egyptologists inspecting hieroglyphs. The biggest underground room, which had formerly housed NATO maps, was three stories high. Xennt was captivated. "I want to be buried here," he said. Van der Loos spent the night in a nearby hotel, but Xennt made a bed in the abandoned map room and slept there.

CyberBunker, a business based near the German resort town of Traben-Trarbach, offered "bulletproof hosting" for Web sites. The air-locked facility, five stories deep, was designed to withstand a nuclear attack.

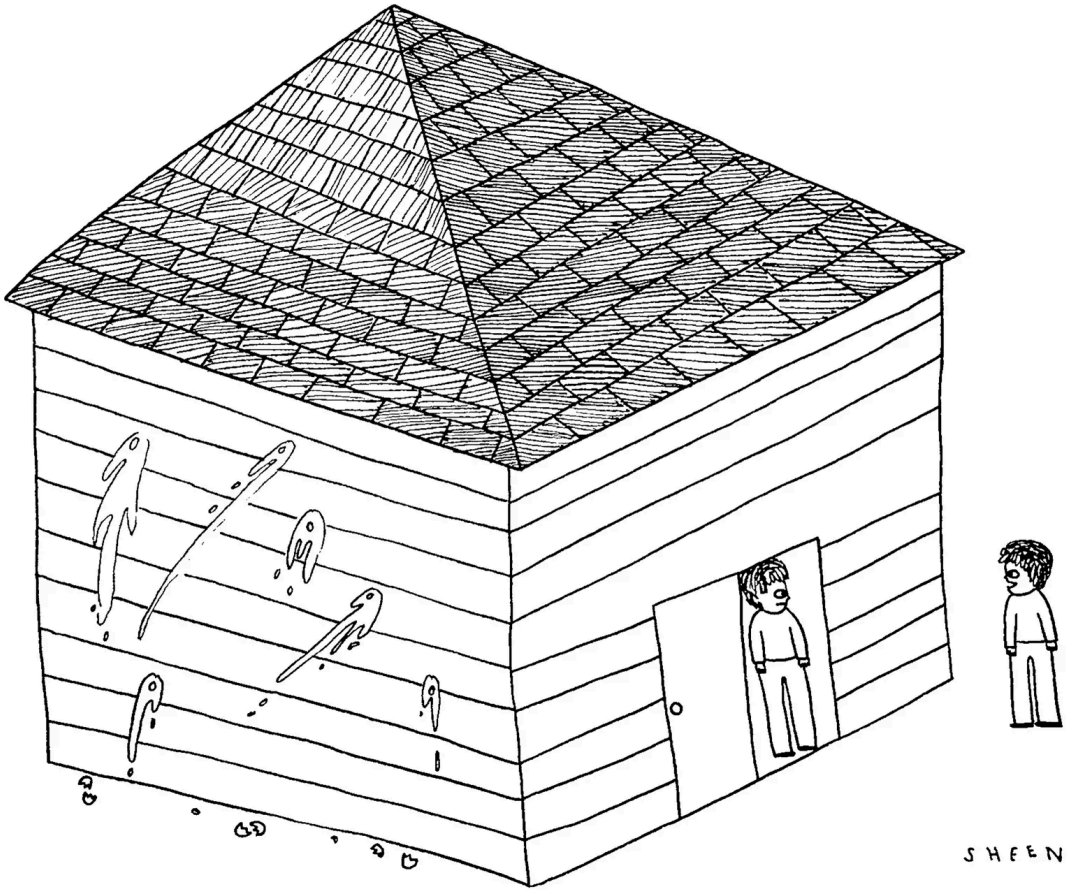
Photo illustration by Max Guther

Xennt moved into the Traben-Trarbach bunker in June, 2013. Angerer kept an eye on Xennt's activities but did not authorize a full investigation of CyberBunker for more than a year. The inquiry presented many legal difficulties. According to German legislation, it's lawful to host a Web site containing illicit material, as long as the hoster is unaware of the content and does not actively assist the site's owner in illegal behavior. Online privacy is an

important principle in German law, and establishing that a hoster knows of or assists in the publishing of illicit content normally requires a communication tap, which a judge is unlikely to permit without prima-facie evidence of criminality. Before Xennt moved to Traben-Trarbach, no Web hoster in Germany had ever been successfully prosecuted.

Michel van Eeten, a Dutch professor of cybercrime at Delft University of Technology, recently helped the Dutch police in an investigation of another "bulletproof hoster," called MaxiDed. The Netherlands has laws similar to Germany's on such matters, and van Eeten told me that investigators were left in "a Catch-22": "We don't have the power to show that the hosters are actively facilitating crime, and so we don't have the power to actually collect the data." Van Eeten told me that the MaxiDed case, which was tried last year, turned on a piece of luck. A separate Dutch investigation of a child-abuse site revealed that it was owned by the same people who owned MaxiDed. The judge in the MaxiDed case then allowed some digital intercepts. In one e-mail exchange, which I have seen, a customer complained that his server had been shut down for "abuse" even though he had paid a premium for permission to host "adult, erotic, movies, doorways, dating, vpn, blogs, xrumer, and zennoposter." (A "doorway" page is a means of manipulating search engines; XRumer and ZennoPoster are tools for spreading spam.) The MaxiDed representative asked the customer what he had been running on his server. The customer responded, "xrumer." The MaxiDed representative said, "OK. Proceed." The customer then acknowledged that he had also used the server as a command-and-control center for denial-of-service attacks. The hoster replied, "Done . . . should be up in a few minutes."

Despite this damning evidence, the MaxiDed case was not easy to prosecute. The company was shut down and two of its administrators were arrested. One was tried in the Netherlands but was convicted only on a single count of money laundering. On all other counts, the prosecutors failed to show that MaxiDed had been a knowing accessory to crime. "The case sort of fell apart," van Eeten told me.



"Do you have any more eggs I could borrow?"

Cartoon by Justin Sheen

Open cartoon gallery

Angerer, the German prosecutor, knew that if he was going to bring down CyberBunker he needed both analog and digital evidence of wrongdoing. After Xennt set up shop in Germany, local police officers started monitoring the property, though they could not see much, because Xennt had added taller fencing to the ramparts, and dogs to guard the perimeter. The officers also enlisted someone connected to CyberBunker as an informant. At the start of 2015, a German cybercrime unit based in the city of Mainz began investigating Xennt's activities.

In December, I travelled to Mainz, which is about an hour east of Traben-Trarbach, and met with the cybercrime team. Three police officers and two civilian contractors worked out of a crowded room in a quiet area of the city.

The unit's headquarters had the ambience of a nerdy frat house. Decorating one wall was a "Breaking Bad" poster featuring the show's antihero, Walter White—a disgruntled chemistry teacher who begins cooking enormous quantities of meth in a high-tech bunker. The officers asked that I not use their names, but they were happy to discuss their five-year investigation of CyberBunker. None of the men looked old enough to have been doing anything professional for half a decade.

The police officers told me that, later in 2015, German authorities granted them permission to intercept the bunker's Web traffic. The officers tapped a cable going into the facility; the inflow and outflow were "mirrored," or copied, but not stopped. A small portion of the information they captured—around ten or fifteen per cent—was unencrypted. On that "clear" portion, the police could see links to illegal Web pages that sold drugs, facilitated credit-card fraud, and conducted other scams. Although the police could not decode any of the encrypted data, the size of the flow suggested that CyberBunker was offering bulletproof protection for a huge number of so-called dark-Web sites. Xennt, in other words, was hosting illicit marketplaces.

Most people use only a fraction of the Internet. A small percentage of Web content is accessed through search engines like Google, or discussion sites like Reddit, or news sites like cnn.com. Beneath the "clear" Web that most people use is a vast amount of non-searchable and password-protected content, including government reports, scientific material, and medical records. This section of the Internet is known as the deep Web. Beneath this level is the dark Web, which exists largely on Tor—software that allows users to communicate with one another without betraying their identities or their I.P. addresses.

Tor is based on technology developed in the mid-nineties by employees of the U.S. Naval Research Laboratory, with the intention of protecting online communications. (Tor is still partly funded by the U.S. government.) The first working version of the software was launched in 2002. Tor's premise is simple and elegant. The Internet works by sending packets of information from one

computer to another. The Tor browser routes all traffic through a network of relay nodes, in such a way that the starting point cannot be detected by the destination. As data pass through each of the relays, encryption is stripped away like the layers of an onion. Tor is an abbreviation of "the onion router."

In repressive states, the dark Web has become a haven for political activists. Many journalists use Tor to send and receive information securely, or to communicate with sources. Some users like the fact that dark-Web pages are not subject to the same censorship as the regular Web, where there are limits on what you can say. Other users appreciate Tor because they can avoid offering up their private data to such giant corporations as Google and Facebook. Some legitimate news outlets, including the *Times* and ProPublica, maintain onion-router pages.

Yet a 2016 study by researchers at King's College London found that sixty per cent of Tor sites contain illicit material. Between 2011 and 2013, the first truly successful dark-Web bazaar, the Silk Road, processed hundreds of millions of dollars' worth of illegal drug transactions. The site, modelled on Amazon or eBay, used the U.S. Postal Service to deliver packages. The F.B.I. eventually closed the Silk Road, and its founder, Ross Ulbricht—an American who went by the online moniker Dread Pirate Roberts—is now serving a life sentence in an Arizona prison, without the possibility of parole. Before his arrest, Ulbricht had espoused a libertarian outlook, and had argued that the Silk Road was forging a path toward a world unfettered by repressive governments. Every transaction on his site, Ulbricht wrote to Silk Road users, weakened "the thieving, murderous" state.

It's easy enough to access Tor. You can download a Tor browser onto a regular computer; or you can run an operating system, funnelled through Tor, from a USB stick plugged into your device. Dark-Web sites look much like the rest of the Internet, but they are generally much more difficult to navigate: you often find yourself scrabbling around like a hiker lost on a trail at night, trying to read a hand-drawn map with a flashlight. If you use a search engine to find a popular dark-Web site, you will see lists of recent links to that site, but some of the links

will lead to error messages. Such addresses are characterized by a mess of numbers and letters, which makes memorizing them virtually impossible. (On Tor, the e-mail and chat provider Riseup appears as http://vww6ybal4bd7szmgncyruucpgfkqahzddi37ktceo3ah7ngmcopnpyyd.onion/.)

I recently spent some time on Dread, a forum accessed through Tor which is a kind of Reddit for the dark Web. In one thread, commenters used assumed names to discuss the selling of illegal drugs in the United Kingdom. They were talking about how the coronavirus outbreak would affect the importation of narcotics. "Would you see any of this moving to more attempts at UK based production?" someone using the handle Darknetpeach asked. "Surely MDMA and pills can be produced on home soil?" CoronaKid, apparently an importer, said, "We'll be fine, shipments will still get thru . . . places like Holland will always be the main players for bulk production. . . . Just stock up now if you're worried." CoronaKid suggested visiting a dark-Web drug exchange, Empire Market, which he said was well provisioned. Darknetpeach was less sanguine, arguing, "100% there will be coke and heroin shortages."

Xennt lived a peculiar existence in Traben-Trarbach. The bunker was not designed with domesticity in mind. The entrance to the complex was through a barrier gate, next to a Bundeswehr-era sign that said "HALT," in giant letters. Inside, Xennt was joined by an ever-changing group of perhaps two dozen people, including programmers and technicians from various European countries, several girlfriends, a gardener, a cook, and, for a period in 2015, Sven Kamphuis. Employees and guests were generally given rooms in the old Nazi barracks, where the cook prepared meals. Xennt liked to tell visitors that the barracks had once housed part of Hitler's eugenics program, but there is no evidence for that claim. There was only one shower in the 1933 structure, and the facilities were rudimentary. Xennt slept in the bunker, on the first underground floor. His bedroom was furnished with black satin sheets, an elaborate sound system, and a life-size figure of the Marvel character War Machine, which stood by his bed.

When Xennt bought the Traben-Trarbach property, he invited his sons, who were now young adults, to work there. Their mother, Angelique, came along, too, though she didn't work at CyberBunker. According to a childhood friend of the sons, who visited the complex, the family didn't fully reunite: Angelique and her sons stayed in the aboveground barracks with the other workers.

People from Traben-Trarbach remember Xennt driving into town in a white BMW X6. When Ajax, Amsterdam's best soccer team, played in the Champions League tournament, Xennt liked to eat pizza at the Costa Smeralda restaurant, then watch the game at a sports bar next door. Sometimes Xennt and his crew visited a strip club in the nearby town of Trier. The staff at the pizzeria and at other local restaurants recall Xennt and his colleagues tipping well. Traben-Trarbach is not a diverse place. Xennt, with his trenchcoat and long yellow hair, stood out, as did his multilingual and multiracial companions. The locals found the group strange but glamorous—like a pirate crew that had unexpectedly docked in town.

A rumor started that Xennt was cultivating cannabis in the bunker, and local people were alarmed by the guard dogs roaming the property. To reassure members of the city council, Xennt occasionally gave tours of the facility. Langer, the mayor who had worked at the complex for the Bundeswehr, visited twice, at Xennt's invitation. He remembers feeling aggrieved that the jobs Xennt had promised for local people had not materialized, but he saw no marijuana cultivation or any other obvious signs of illegal activity.

The bunker had not changed much since Langer had stopped working there, except that the grounds were a lot messier. There was the same color-coded scheme for differentiating floors. Old maps of Afghanistan hung on the walls. On the fifth level down were the water tanks. On the fourth level down were the generators. On the third level down, an old supercomputer used by the Bundeswehr was still hooked up to a giant screen. On the same floor, a room was filled with racks of Dell computer servers. The heat from these servers warmed the whole bunker, through the air-conditioning vents.

"There was always this funny feeling—what was on those servers?" Langer told me. "And Xennt would say, 'That's my customers' secret.' "

When Frank Van der Loos, the Dutch programmer, first visited the bunker complex, in the fall of 2015, he was bowled over by how enormous the property was. He was on the site for two days, and saw "maybe a third of it." Xennt told Van der Loos that he kept finding new rooms.

Van der Loos also wondered what was on those servers. In 2014, Dutch authorities investigating the dark-Web marketplace Cannabis Road had seized a CyberBunker server housed in Amsterdam, at a facility owned by the company Leaseweb. A Dutch prosecutor explained that the server had been impounded because Xennt was suspected in the trafficking of drugs. Xennt reassured his colleagues at CyberBunker that he had merely leased the impounded server, and hadn't known what it was used for—a legitimate position, under both Dutch and German law. Xennt told Van der Loos that the Traben-Trarbach servers were, in a similar way, closed books to him. Nevertheless, he felt that he was being spied on by the German police. "I don't do anything wrong," Xennt told Van der Loos. "Still, they are watching me."

Van der Loos was surprised to see that Xennt's office was littered with phones—there were around thirty modified BlackBerrys on his desk alone. Xennt explained to Van der Loos that the phones were why he had been invited to Traben-Trarbach. He was expanding into an exciting new business.

Bulletproof Web hosting had originally been lucrative, but by 2015 most legitimate sites had migrated to conventional hosters, and competition had driven rental prices down, making the business model less viable. Xennt's server business generated annual profits of between two and three hundred thousand euros—enough to cover the maintenance costs of the bunker, but not much more. (According to USENIX, a nonprofit that studies computing systems, MaxiDed, the Dutch bulletproof-hosting service that was shut down, accrued profits of no more than six hundred and eighty thousand euros in seven years,

whereas a child-pornography site that it hosted made more than four million in five years.) Xennt told Van der Loos that he was turning over the day-to-day supervision of CyberBunker's servers to his eldest son. Xennt's new project was building an encrypted-phone network, which he called "a money-maker." He asked Van der Loos to help him.

"I didn't want to embarrass them by telling them I don't work here, so I told them it was a three-hour wait for a table instead."

Cartoon by Carolita Johnson

Open cartoon gallery

Around the time of Van der Loos's visit to the bunker, Nicola Tallant, an Irish crime reporter from the *Sunday World*, also arrived in Traben-Trarbach. She has a reputation for writing juicy, exclusive stories about Irish criminals. In 2015, she received a tip from a source that a major Irish drug dealer, George Mitchell, had moved from southern Spain to Traben-Trarbach, in order to work on an encrypted-phone business with Xennt. She had never

heard of Xennt, but a tourist town in the Mosel Valley is a curious headquarters for a crime boss, and so Tallant decided to investigate.

Mitchell has a portly frame and a distinctive waddle, and is sometimes known as the Penguin. Whenever he visited CyberBunker, he went by Mr. Green. By the mid-nineties, he had become one of Ireland's most successful importers of illegal drugs. But he abruptly left for Amsterdam after he was linked to the attempted murder of a London gangster and to the creation of Ireland's first Ecstasy factory. In 1998, Mitchell was arrested in the Netherlands after he was caught unloading a shipment of stolen computer parts, and he spent a year in jail. According to a senior Irish police detective, Mitchell's drug-importation business thrived even after his Dutch jail term; in 2012, he facilitated the attempted shipment to Ireland of some four hundred kilograms of cocaine—an operation thwarted by the police. The detective told me that Mitchell remained a major figure in the European drug trade until about six years ago. "From '14 or '15 onward, we didn't see much from Mitchell in terms of the importing of drugs," he said. "It may be that he branched out into other areas." (In fact, European police intelligence suggests that Mitchell continued to organize large shipments of drugs after 2014. Mitchell has denied any involvement in criminal activities.)

Tallant had her own theory about the Penguin: he was approaching retirement age, and, as the father of several children, he was looking for a way to protect his dependents and his assets. In 2000, his son-in-law, a drug supplier named Derek (Maradona) Dunne, was murdered in Amsterdam. And around the time Mitchell arrived in Traben-Trarbach a dispute among Irish gangs had turned bloody. In September, 2015, Gary Hutch, an Irishman who had previously worked with Mitchell, was killed by a rival group on the south coast of Spain. Mitchell, Tallant surmised, wanted to leave Spain and the gang feud behind, and to reinvest some of his money in a more legitimate-seeming enterprise.

Mitchell had known Xennt for many years, at least from the time of Mitchell's arrest for handling stolen computer parts, in 1998. (A person familiar with Xennt's computer business told me that Xennt had bought stolen parts from

Mitchell; Xennt declined to comment on this accusation.) Martijn Burger, the businessman once involved in the Public Root movement, remembers Xennt and Mitchell spending time together around the turn of the millennium. Back then, Burger did not know of Mitchell's status in the criminal world, and teasingly called him Charlie Chaplin, because of his gait. Burger recalled that Mitchell was often accompanied by glamorous young women, and carried a small bag containing "ten to twelve" Nokia phones, each with its phone number written on the back.

When Tallant received her tip, Mitchell had not been photographed in more than two decades. She travelled to Traben-Trarbach twice in the fall of 2015, along with a *Sunday World* photographer. They watched his movements for several days. He rarely left the apartment complex where he was staying, on the Traben side of town. But on some mornings Xennt picked up Mitchell and took him to breakfast. The pair once ate lunch at a popular local restaurant, the Historische Stadt-Mühle—the Historic Mill. They remained there all afternoon as Mitchell ordered gin-and-tonics and Xennt drank hot chocolate. Tallant was fascinated by Xennt's appearance: he often wore a floor-length coat, and resembled a Bond villain. "He is *sensational*-looking," she told me. "I've never seen anyone as weird in all my life."

Tallant and the photographer eventually found their opportunity one morning, as Mitchell was leaving a restaurant after having breakfast with Xennt and Xyonn. The Penguin wore a navy suit and a black T-shirt; Xennt had on a long black puffer jacket; Xyonn had his hair in dreadlocks.

Tallant walked up to Mitchell and said, "George, quick word—how are you?"

"Very good," Mitchell replied instinctively, in his broad Dublin accent. Then, surprised at hearing another Irish voice, he peered under the baseball cap that Tallant was wearing, and evidently recognized her. "Fuck off!" he said.

The photographer got his shot. Tallant's exclusive was published the next Sunday, under the headline "THE LOST GODFATHER."

The encrypted-phone business is indeed a money-maker. Many people now use end-to-end encrypted-communication apps like Signal and WhatsApp on their smartphones. But, for a small subset of privacy-minded people, such apps are insufficient: they want a specialized, fully encrypted phone that operates on a private network. A "crypto phone" normally costs a user between fifteen hundred and two thousand euros for the handset, and biannual payments of up to a thousand euros for access to a private data network. The handsets—often reëngineered Android or BlackBerry devices—tend to be sold with the camera, the microphone, and location services disabled. The phone typically uses only one end-to-end encrypted-messaging app, which runs on servers that the providers own. Many phones include a panic button that wipes all data from the handset when activated.

Providing or using an encrypted phone is not illegal in Europe or in America, but the devices appear to be used predominantly for illegal activities, and prosecutors have begun finding ways to break up some encrypted networks. In March, 2019, the U.S. Attorney for the Southern District of California brought racketeering-conspiracy charges against Vincent Ramos, the C.E.O. of a Canadian company called Phantom Secure. Six months later, he pleaded guilty to "leading a criminal enterprise that facilitated the transnational importation and distribution of narcotics through the sale of encrypted communication devices and services," and was sentenced to nine years in prison. Many of Phantom Secure's customers were members of the Sinaloa drug cartel, in Mexico. It was the first case in the United States in which an encryption-service provider was jailed.

One of the best-known private phone networks is one that collapsed. In April, 2016, Danny Manupassa, the owner of a Dutch company called Ennetcom, was arrested, on suspicion of money laundering and possession of illegal weapons. The servers used by his network, which were housed in Toronto, were seized by Canadian authorities and passed on to the Dutch. Officials in the Netherlands were able to decrypt many communications by Ennetcom users, likely because the company had housed decryption keys on the same server where it stored

messages—a catastrophic error. By 2017, the Dutch police had decrypted 3.6 million messages. Several people have since been arrested because of this trove of criminal evidence, including Naoufal Fassih, a Moroccan-Dutch gangster, who was sentenced to eighteen years in prison for attempted murder. (In early July, Dutch, British, and French police announced that they had infiltrated another popular network, EncroChat. This had led to more than eight hundred arrests, across Europe, and to the seizure of huge quantities of guns and drugs—and of some sixty-seven million dollars in "suspect cash.")

In Traben-Trarbach, Xennt built his own encrypted-phone network and applications with the help of Sven Kamphuis and some programmers in Poland. Xennt explained to me that his apps are "sold and distributed under various brands all over the world, by third parties." One of the first encrypted-phone apps that Xennt developed, called Underground, was sold on a modified BlackBerry handset. More recently, he developed a messaging app called Exclu, which uses a novel encryption scheme and is sold on a Wileyfox Android device.

Many of Xennt's initial encrypted-phone customers were in Ireland; his market subsequently spread throughout Europe. Xennt told me that his phone business was more lucrative than his hosting business, although the extent of its profitability is hard to assess without seeing a balance sheet. The F.B.I. reported that Phantom Secure, the company that had facilitated the Sinaloa cartel, had earned annual revenues of eighty million dollars, but that network had between ten and twenty thousand devices—at least twice as many as Xennt's—and server infrastructure on four continents; it also charged a much higher biannual renewal fee. The yearly profits of Xennt's phone business likely never went much beyond a million dollars.

During Frank Van der Loos's 2015 visit to the bunker, Xennt asked him to help develop software for his phones that would include the ability to send money to other users of the private network. According to a former colleague, Xennt also wanted to include a "back door," so that if a phone was seized, or the network was disabled, Xennt could drain all the funds stored in the application's escrow

account. Van der Loos refused, on ethical grounds. (Xennt told me that he never would have asked for a back-door feature, because it clashes with his "views on privacy.")

According to two people close to CyberBunker, George Mitchell was not the only investor interested in Xennt's encrypted-phone business. Danny Manupassa, the former boss of Ennetcom, also travelled to Traben-Trarbach to see Xennt. According to the sources, Manupassa wanted to invest a million euros in Xennt's network. It seems unlikely that Manupassa did so: after he was arrested, in April, 2016, Ennetcom was shuttered and turned inside out by the Dutch police in a search for information.

The German police's interest in CyberBunker intensified after the sighting of Mitchell in 2015. They suspected that he might be the guiding figure behind a large criminal enterprise, based in the bunker. A judge allowed the police to tap sixteen of Mitchell's non-encrypted phones. But, despite glimpses into his criminal dealings, including mentions of shipments of "oranges"—which the police assumed was a coded reference to drugs—there was never enough evidence to charge Mitchell with a crime. In 2016 or 2017, perhaps sensing that he was being watched, he left Traben-Trarbach. Mitchell's most obvious role before then was as a salesman for Xennt's encrypted-phone business, which he marketed to members of Colombian drug cartels and to biker gangs in Majorca. "It's the only way, all my friends use it, everybody," he told a prospective client on a recorded call.

The police unit in Mainz decided to focus on CyberBunker activities that were provably criminal. Running an encrypted-phone network is not illegal, even though it very often brings providers into contact with known criminals. Similarly, hosting dark-Web sites is not against the law. But if police officers could demonstrate that Xennt and his team were actively assisting the administrators of dark-Web sites that traded in illicit substances or services, they could build a strong case against CyberBunker. Conveniently, Xennt's operational security was often poor. In the early days at Traben-Trarbach, he

and his team occasionally used unencrypted e-mail, which the police were able to monitor. But the authorities needed a better way to establish the relationship between Xennt and his dark-Web clients.

The cybercrime unit developed a bold scheme. With the permission of high-level German authorities, it created its own dark-Web site on Tor: a scam, involving lottery numbers, that accepted payment in bitcoin. The unit's members made sure that nobody who used the site could lose money—otherwise the officers themselves would be committing a crime—but the site was designed to look as realistic, and as shady, as possible. Designing it was "kind of fun," an officer admitted to me.

"And isn't it true, Mr. Robertson, that you habitually leave ridiculously small amounts of cereal in the box and then return it to the cabinet?"

Cartoon by Teresa Burns Parkhurst

The Mainz team members received permission from their superiors to buy thousands of dollars' worth of bitcoin, then e-mailed CyberBunker, asking to rent a server. A representative from the company readily agreed, and the undercover officers engaged in a long dialogue with a CyberBunker salesperson. The officers would not share details of that discussion with me, because it would reveal "police tactics," but they ascertained that Xennt's company actively assisted clients it knew to be engaged in illicit transactions. CyberBunker even offered some clients tips for hiding their real identities.

The police, meanwhile, began ensnaring Xennt in a more direct fashion. When Frank Van der Loos visited the bunker in 2015, he chastised Xennt for using cheap technology that compromised his operational security. Xennt's servers were not connected by a virtual-LAN cable, which allows the digital traffic from individual servers to remain separated, even if the servers are using the same physical cable. Van der Loos told me that if someone wanted to "listen" to the activity on CyberBunker's servers, all it took was secretly adding another server to the group. Separately, I learned that in 2018 a young intern at CyberBunker discovered a server on the third floor which looked nothing like the others. Hidden underneath the floorboards, it was connected to the rest of the server bank. When I asked the leader of the Mainz team whether he had asked an informant working in the bunker to install the extra server, as a spying device, he stifled a laugh, then said, "I cannot answer it, and I cannot deny it." (Xennt told me it was "impossible" that the police had surveilled him in this way.)

By various methods, the police came to believe that CyberBunker was the biggest hoster of illegal Web sites in Germany, and perhaps anywhere in the world. In 2014, it hosted Cannabis Road, the dark-Web marketplace. Between March, 2016, and February, 2018, it hosted the forum Fraudsters, through which counterfeit money, fake I.D.s, and prescription and illicit drugs were traded. Between 2015 and 2018, CyberBunker hosted Flugsvamp, a dark-Web market that accounted for roughly ninety per cent of the online illicit drug trade

in Sweden. Xennt's most significant dark-Web client was a site called Wall Street Market. Between 2016 and 2019, it sold more than thirty-six million euros' worth of drugs. The site's administrators took a commission of three per cent on each transaction.

While the Mainz cybercrime unit was building its case against Xennt, a separate international investigation—led by federal police in the United States, Germany, and the Netherlands—targeted Wall Street Market. Jörg Angerer, the Koblenz prosecutor, told me it was vital that the prosecution of Wall Street Market proceed before the German police moved against CyberBunker. "There is a chain," Angerer said. "The hosters are facilitating the real criminals. . . . But first you have to process the real criminals."

In April, 2019, the police arrested three German men accused of being Wall Street Market's administrators. On the dark Web, the defendants were known by pseudonyms: Tibo Lousee was coder420; Jonathan Kalla was Kronos; Klaus-Martin Frost was TheOne. Led by officers from Germany's federal cybercrime unit, which is based in Frankfurt, the police in the three countries worked together to decipher the identities of the administrators, through undercover chats and through clues left by the men online. In a complaint filed in the Central District of California, the three principals were charged not only with running the site but also with planning an "exit scam," in which they intended to abscond with some eleven million dollars being held in users' accounts. All three men are awaiting trial.

A week after Wall Street Market was broken up and its leaders arrested, several officers from the B.K.A., Germany's federal police force, arrived at the Traben-Trarbach bunker to seize evidence relating to the case. A manager at the bunker expressed surprise and readily complied, escorting the officers to the server bank on the third floor. The officers took away the servers used by Wall Street Market, and left the rest.

After Wall Street Market was taken down, Angerer fixed CyberBunker itself in his sights.

On September 26, 2019, everybody at the bunker complex—nine people, including Xennt, his sons, and his girlfriend, Jacqueline—went out for an early dinner at the Historic Mill, leaving the bunker unguarded. It was unusual for all the residents to be gone at the same time, but Xennt's gardener, Harry, had unexpectedly come into an inheritance, and wanted to celebrate. The leader of the Mainz cybercrime team told me his unit had gathered intelligence that made them "pretty, pretty sure" nobody would be in the bunker during the meal.

At the Historic Mill, antiquated cooking utensils and old guitars hang on the walls. Through a glass panel on the floor, diners can look at the stream that once powered the old mill. Xennt's group had booked a private area on the mezzanine. It was a Thursday evening at the end of the summer season, and the main dining room, on the ground floor, was nearly full. At around 6 P.M., as the members of Xennt's party were starting to eat, several patrons on the ground floor revealed themselves to be armed undercover police officers. The officers went upstairs to arrest Xennt and the others. Several armed units of police massed outside the front door. A helicopter buzzed nearby. A Belgian tourist was almost caught up in the arrest when he tried to visit the bathroom on the mezzanine just before Xennt was placed in handcuffs.

A few minutes later, about a hundred police officers—including a contingent from Germany's federal paramilitary police unit—raided the bunker. They seized four hundred and twelve hard drives, four hundred and three servers, sixty-five USB sticks, sixty-one laptops and computers, fifty-seven phones, piles of paper documents, and about a hundred thousand euros in cash. Some six hundred and fifty officers were involved in the arrests and the raid.

At a press conference the next day, German authorities were jubilant. Jürgen Brauer, the chief prosecutor, declared that it was the first time in German history that arrests were "not directed against the operators of marketplaces but against those who make the crime possible." CyberBunker was a haven for the world's worst dark-Web sites, established to help its clients "exclusively for illegal purposes." Moreover, its operators were connected to people involved in

organized crime. (Brauer didn't name the Penguin—whose current location remains unknown—but he was clearly in his thoughts.) Xennt had been arrested, alongside his two sons, Jacqueline, two Germans, and a Bulgarian. Six other suspects remained at large.

The prosecutors reported that, in November, 2016, the bunker had also provided the command-and-control servers for an attack against Deutsche Telekom, one of Germany's largest communications companies. The attack had deployed a new weapon called a Mirai-botnet, which harnesses smart appliances and other wireless devices. An attempt to capture the company's routers failed but caused the network to crash. More than a million Deutsche Telekom customers lost their Internet connection in the attack, costing the company at least two million euros. The incident occurred only a few weeks after an even larger Mirai-botnet attack in Europe and the United States, which disabled Amazon, Netflix, and Twitter, among other sites. Brauer, the prosecutor, said that the people from CyberBunker who had been arrested were accused of "hundreds of thousands of offenses," ranging from "drugs, counterfeit money, and forged documents" to being "accessories to the distribution of child pornography."

Sven Kamphuis, the Prince of CyberBunker, was not arrested in the raids of September 26th; nor is he one of the six suspects still at large. After the raid, he claimed that the German police had engaged in "an act of war"—yet he had survived with barely a scratch. The police arrested almost everybody with a connection to the bunker. Given the comprehensiveness of the investigation, the prosecutors' lack of interest in Kamphuis seemed strange.

Xennt insisted to me that Kamphuis "was not involved in the data center in Germany." But Kamphuis told me that he had engineered much of the Traben-Trarbach bunker's infrastructure, and, according to several people, he had also been important in developing the encrypted-phone business for Xennt. Even if Kamphuis's work was not technically illegal, he was deeply knowledgeable about an organization that the German state believed to be criminal. When

details of an indictment were published, in April, the mystery of Kamphuis's treatment deepened. In the document, prosecutors noted that a search engine had been hosted on the Traben-Trarbach servers: cb3rob.net/darknet. It listed more than sixty-five hundred dark-Web sites, including "marketplaces for narcotics, weapons, counterfeit money, murder orders, and child pornography." I recalled that CB3ROB is Kamphuis's online handle.

When I asked Patrick Fata, a senior police officer who oversaw the CyberBunker investigation, why Kamphuis was not accused in the case, he said that Kamphuis's role in the organization had diminished since 2014, and that the police did not have enough evidence to link him to the administration of Wall Street Market or other illegal sites. I asked Fata if the police had spoken to Kamphuis during the exhaustive six-year investigation. "No," Fata said, adding, "We don't know where he is."

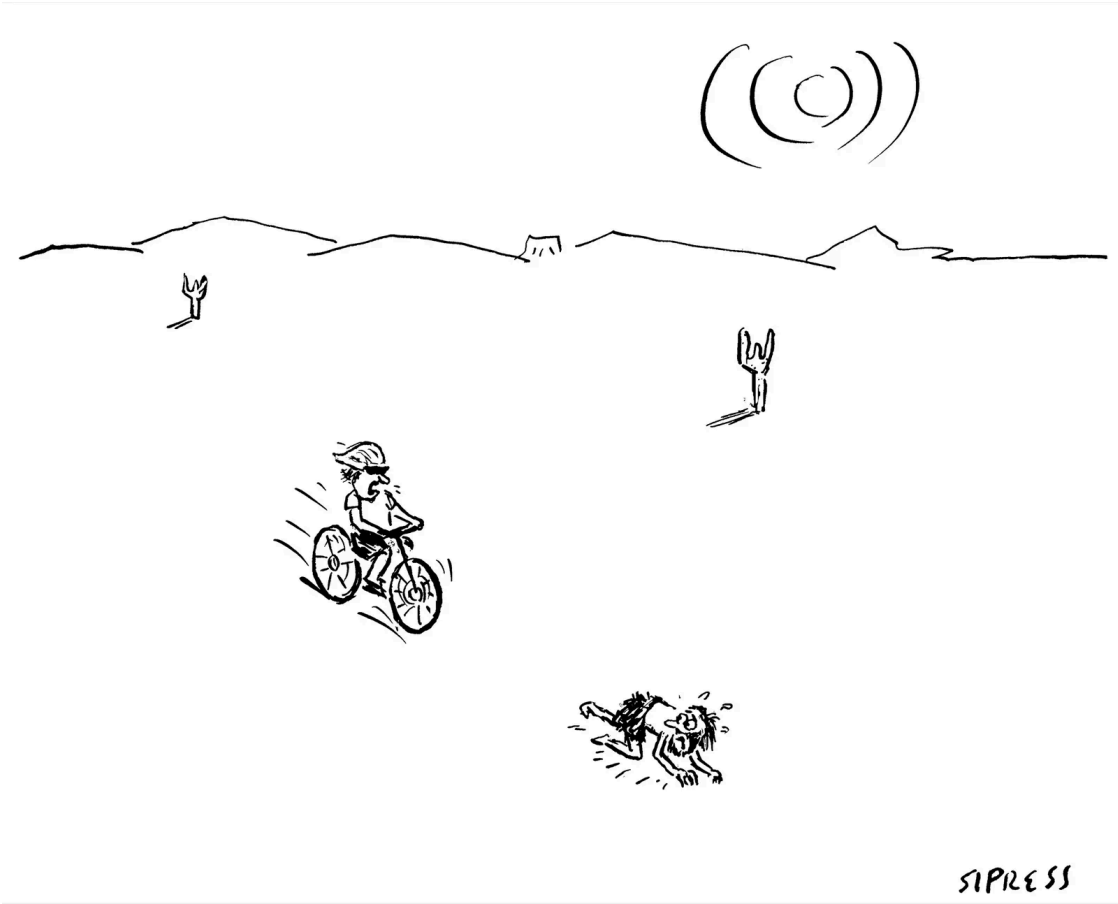
It was surprising that the German police, who had proved so competent in this investigation, had lost track of Kamphuis. After his arrest for the denial-of-service attack on Spamhaus, in 2013, he had spent fifty-five days in a Spanish jail while awaiting extradition to the Netherlands. Ultimately, a judge had placed him on probation for two years. The German and Dutch police coöperated extensively in the early days of the investigation into CyberBunker, and during Kamphuis's probationary period it would have been easy enough to place legal pressure on him to talk to the German police.

I found Kamphuis without too much difficulty. He agreed to meet me in March, in a train-station café in Middelburg, a pretty Dutch city near the first CyberBunker site. Kamphuis, who was wearing a blue Adidas tracksuit, had piercing blue eyes and a scraggly beard. Some of his teeth were blackened, and a few were missing. Using a tissue, he frequently dabbed at pus weeping from a sore on his eyelid. He drank three strong coffees in about ninety minutes, and his hands kept shaking.

Kamphuis posts on the social-media site Gab, and his stream is a litany of conspiracy theories and anti-Semitic assertions. He told me that he was part of the "libertarian extremist right," and suggested that a "disproportionate number

of Jews" held powerful positions in Europe and America. He often laughed at his own jokes.

I asked him if he had created the dark-Web search engine that had been hosted on Xennt's servers. He said yes. Later, by text message, he explained that he bore no responsibility for the results of the search engine, because it "finds things indiscriminately," adding, "That is what search engines do."



"Hey! You're in the bike lane!"

Cartoon by David Sipress

Open cartoon gallery

Kamphuis insisted that he had not been an informant against Xennt. He accused a manager at CyberBunker, Tom Funken, of planning the dinner trap at the Historic Mill—even though I had been assured by Xennt's family that the meal was a setup arranged by the gardener. Xennt told me that he also blamed

the gardener, and maintains that there were "no informants" inside the bunker. (Funken was arrested and awaits trial. A recently leaked legal file suggests that, between 2018 and the raid, the gardener was an undercover policeman.)

Although Kamphuis said that he hadn't been involved regularly with CyberBunker since 2014, he still considered himself "the prince, and currently the head of state," of the organization. He felt under no legal pressure, he said, because both Spain and the Netherlands "respected his diplomatic immunity." Kamphuis inveighed against the German police, but he appeared to have profited from their prosecution of Xennt: he said that he was now helping to run Xennt's encrypted-phone business, which had not been shut down.

After our interview, I texted Kamphuis, and asked him again if he'd ever spoken to the German police. "We don't negotiate with terrorists," he said.

Xennt has been imprisoned in Koblenz since his arrest. Although his lawyer would not discuss a legal strategy, Xennt's defense appears to be that he didn't know what was on his servers. He told me, "I do not believe that a hoster should accept all kind[s] of content. . . . As soon as a hoster [has] a clear indication that illegal content is hosted then the hoster should cancel the service." CyberBunker's willingness to hand over the Wall Street Market servers might buttress that defense. However, a report by *Der Spiegel* claims that, a day after his arrest, Xennt became emotional and apologetic in a police interview, saying that he was "troubled" by how much illegal activity had flowed through the bunker.

Xennt won't stand trial until this fall at the earliest, because of delays caused by the coronavirus crisis. Even then, prosecutors will have an incomplete picture of what went on in the bunker. Since the raid, analysts have attempted to sift through the data stored at the facility, which may amount to two thousand terabytes—a herculean task. It would take a large team many years to read a fraction of what was recovered in Traben-Trarbach. In April, however, the

prosecutors said that they had identified dozens of CyberBunker clients—and not one of their enterprises was legal.

I wondered what good would come of all the data. A spokesman for the German federal cybercrime unit that led the international investigation into Wall Street Market told me frankly that the war against dark-Web bazaars was unwinnable. Just as Wall Street Market had flourished after the Silk Road's demise, new markets would grow in the place of Wall Street Market. People would continue to have illicit desires, and the Internet would find ways to satisfy them. Nevertheless, the penetration of the Traben-Trarbach bunker had offered valuable insight into how nefarious elements operated online. "I do not recall any case where this huge amount of criminal-infrastructure data was gathered," one of the officers in Mainz told me. "We want to learn how the other side is behaving."

Xennt was formally indicted on April 6th. German authorities stated that he had "made all the business decisions" for CyberBunker, and described him as the head of a "criminal organization." This depiction was a bit difficult to square with the stranger, more complex reality of Xennt. A patina of idealism, however misguided, seemed to be essential to him. A police officer who monitored him for several years said that Xennt's seedier qualities were accompanied by a utopian outlook—"free Internet, freedom of speech, nobody controls what's out there, stuff like that." The officer conceded, "This is no bank heist. It's not like he's a billionaire."

In March, I visited Xennt's sister and brother-in-law, Anna and René Van Wolferen, in a village near Arnhem. The Van Wolferens have a tidy, well-appointed home, with a wood-burning stove in the sitting room. René works for a pharmaceutical company and is an auxiliary firefighter. He wore a beeper on his belt, and a T-shirt with the slogan "We Face What You Fear." Anna is a tall woman with auburn hair and a friendly, anxious manner. They showed me an Exclu phone that Xennt had sent them from the bunker. Neither of them

had ever unwrapped it; to show me how it worked, they had to charge it for twenty minutes.

The Van Wolferens explained that Xennt had always lived "on the edge," but was hardly a cackling mastermind. (The *Sunday World*, the Irish tabloid, recently called Xennt the "lord of the darknet.") Rather, he was a brilliant, dreamy, somewhat naïve person, who had swum out of his depth. They worried about his state of mind in prison, where he played chess against himself all day, and had almost no contact with the outside world. Xennt and Anna's father died in January, and Xennt's lawyer had asked permission for her client to attend the funeral. The request was denied. Xennt then asked for a laptop to watch a live stream of the service, and this was also refused.

The Van Wolferens spoke again and again about Xennt's childhood bedroom in Arnhem, and how he had always been fascinated by a futuristic aesthetic. René said that, in late middle age, Xennt had begun dabbling in cannabinoid treatments, because he was interested in remaining "forever young." He described his brother-in-law as someone with arrested development. "His *whole world* was science fiction," René said.

This was an astute observation. People connected to CyberBunker spoke about the world purely in terms of what was online. They didn't talk about the Netherlands, a country of seventeen million people. They called it by its domain name: ".nl." Similarly, they spoke of "kinderporno," an Internet term for child pornography. In many jurisdictions, there is no such thing as child pornography; any image of a child having sex is considered evidence of abuse. It was in Xennt's commercial interest to ignore the link between the three-dimensional world and what appeared on computer screens. But his many years in windowless rooms may have blinded him to the link altogether. When I asked Xennt if CyberBunker knew that it was hosting the Pirate Bay, the content-sharing site, he responded with the kind of dodge that could be applied to even the darkest material: "If a customer does not reveal its name to CyberBunker, then the CyberBunker crew does not know who the customer is."

When Anna was out of the room, René admitted that Xennt had apparently sometimes gone "over the edge." For reasons that were unclear to René, Xennt often hid his business interests behind charitable foundations. The Van Wolferens' home was listed as an address of one of those foundations. As a result, the couple had been visited more than once by the Dutch police, who asked René about illegal content hosted on CyberBunker's servers. And an Irish criminal connected to Xennt's phone business had once arrived at the Van Wolferen home. René recognized him as a gangster of some kind, and ejected him. René was fond of his brother-in-law, but he told him that his businesses led him to mix with "people who are not legal."

In April, I wrote a letter to Xennt in prison, which was delivered by his lawyer. The sole condition of our correspondence was that we could not discuss matters that might directly affect the trial. Xennt replied to me in May. He wrote in English, in blue pen, on grid paper. His writing was capitalized, except when he used the word "I." He told me he believed that the authorities had targeted his hosting business as a means to "stop the development of the secure communication app." He added, with a few misspellings, "The next version would have a wallet that would have enabled its users to make unlimited instand anonymous payments. That—of corse—would not make authorities very happy." Xennt was passing the time by writing a book about "privacy and what happened to me." He said that he had already "sold the exclusive rights to a movie studio." (I could find no evidence of this.)

In my letter, I asked Xennt about the infatuation that had dominated his unusual life: bunkers. He told me about his childhood visits to the Second World War complex in Arnhem, and about how that space had bewitched him. "I instantly fell in love with it," he recalled. He said that the first CyberBunker, in Goes, was the realization of "a dream" to own "one of these facilities and to renovate it to make it a modern hi-tech stronghold." But he could go no deeper. Xennt wrote, "I am unable to explain why I like bunkers. Why does someone like a hamburger? Why do they like motor sport? I cannot answer that. I just like bunkers. That is all." ♦

An earlier version of this article misidentified West Germany's armed forces.

Published in the print edition of the August 3 & 10, 2020, issue, with the headline "Underworld."

Ed Caesar is a contributing staff writer to The New Yorker. His most recent book is "The Moth and the Mountain."

More: Technology Crime Internet Federal Bureau of Investigation (F.B.I.) Russia Germany Underground Security Dutch Cybercrimes Criminals Computers

READ MORE

THE NEW YORKER DOCUMENTARY

A Couple Faces the Questions Posed by Male Infertility